protiviti®
Face the Future with Confidence

取締役会のリスク監視：Risk Oversight

サイバーリスクに対する取締役会のリスク監視

取締役会は、情報システムのセキュリティと利用可能性、および組織が巻き込まれている商業上のサイバー戦争から機密情報やセンシティブな情報を保護することに関心を持ち続けています。多くの経営者は、自社のリスク許容度は低いと考えていますが、あたかもリスク許容度が高いかのように行動しているため、取締役会がサイバーセキュリティに関与することが不可欠となっています。

ISSUE 90

サイバーリスクは、多くの業種、多くの組織において重要リスク上位5位の1つとして認識されています。[1] 組織が、大規模なITトランスフォーメーション、クラウド・コンピューティングの加速、デジタル化投資の増加[2]、先進的なデータ・アナリティクスの高度化、およびモバイル・デバイスの利用拡大により、コンピューターの処理能力の急激な増大を活用し、競争優位を得ようとする中で、サイバーリスクへの対応は常に移動する目標を捉えるようなものです。これらの革新的なITトランスフォーメーションの取り組みは、デジタル化領域を拡大させ続けており、この拡大は企業が実施しているセキュリティ保護領域を凌駕しています。このジレンマは深刻な現実を表しています。セキュリティとプライバシーに関するリスクを受容可能な水準まで低減する上で有効な内部統制の仕組みは、将来的には不十分となることが避けられず、それも多くの人々が認識しているよりも近い将来においてです。事実、組織のセキュリティとプライバシーは既に侵害されていても、そのことに気が付いていないだけかもしれません。取締役会は、変わり続けるサイバー脅威に直面する中で、自らの組織がサイバーセキュリティ能力の継続的改善を行うことを確実とする必要があります。

主要な考慮事項

プロティビティが行ったリサーチは、情報セキュリティに関する取締役会の関与が改善してきていることを示しています。[3] 以下では、さらなる改善を行うために、取締役がサイバーセキュリティリスクの監視において考慮すべき、企業が置かれている8つの現実を示します。

1. **組織は成功に向けた準備ができていなければならない**：サイバーセキュリティの管理は、よからぬことが起こるリスクを管理するというだけではなく、デジタル化の動きを企業が成功裏に実施することによるプラス面を確保することでもあります。企業がデジタル化とビジネスモデルの革新を通じて新たな価値の源泉を手に入れる中で、企業全体にわたってセキュリティとプライバシーに関する能力を成熟させるためのさらなる進歩が必要とされています。取るべき賢明な進路は、信じがたいほどの成功を前提として計画を策定することです。取締役は、組織のサイバーセキュリティに関する方針とシステムが、そのような成功に対応できるほど十分なレジリエンスを有していることを確実とすべきです。

2. **企業のセキュリティとプライバシーは既に侵害されているが、そのことに気が付いていない可能性は高い**：これまでは、「サイバーリスク事象は発生するか否かではなく、いつ発生するかの問題である」と言われてきましたが、これは過去のものになろうとしています。サイバーリスク事象は、今まさに発生しているのです。多くの企業において、サイバーリスク事象は既に発生しており、今も発生し続けているかもしれません。しかし多くの組織は、必要とする先進的な検知・対応能力を有していません。データプライバシーに関する多くの規制が世界中で制定され、政治家や政府機関、グローバル金融機関、主要な小売業者、その他の著名企業におけるデータ侵害が世の注目を集

1 Executive Perspectives on Top Risks for 2017, Protiviti and North Carolina State University's ERM Initiative, 2017 (www.protiviti.com/US-en/insights/protiviti-top-risks-survey)

2 「デジタル化」とは、業務プロセスの改善を目的として、アナログのソース資料をデジタル様式に変換するプロセスです。

3 Managing the Crown Jewels and Other Critical Data, Protiviti, 2017 (www.protiviti.com/US-en/insights/it-security-survey)

めていることを受けて、取締役と経営者も、レピュテーションとブランドイメージを保護するために「サイバーレジリエンス」が必要であることを認識するようになりました。

取締役会は、重大な侵害が、最終的に検知されるまで、どの程度の期間にわたっていたのかについて関心を寄せるべきです。プロティビティの経験では、多くの業種において検知とモニタリングを行う統制は成熟度が低いままであり、適時に侵害を検知できない状態が続いています。机上の演習のみでは、侵害者の高度化と侵害の重大な影響への十分な対応を行うことはできません。想定される攻撃のシミュレーションを定期的に実施し、侵害の検知と適時の対応を確実とすべきです。加えて、サイバーリスク事象の影響と拡散を低減するための組織の準備度合いが重要となります。従って、取締役会は、インシデント発生後の対応、復旧、および通常業務再開の手順の十分性に対して焦点を当てるべきです。その手順には、侵害に伴って起こり得るレピュテーション被害を最小化するための、顧客と従業員への対応を含めるべきです。

3. **取締役会は不利な事業上の結果とその管理に焦点を当てるべきである**：ほとんどの企業は、最も重要なデータ資産と情報システムが何であるかを把握しています。しかし、セキュリティリスクを評価する際に、管理しようとする事業上の結果に焦点を当てることが忘れられています。リスク発生による結果またはシナリオを検討することにより、特定の資産やシステムに焦点を絞った対応よりも、より包括的な全社的セキュリティ・ソリューションが導き出されます。

例えば、あるアプリケーションが事業の成功にとって重要であると判断された場合、それを管理の対象範囲に含めることが通常です。リスクがセンシティブなデータの漏洩に関するものである場合、データ元のアプリケーションに焦点を当て、汎用的なセキュリティ統制を実施することが、セキュリティ・ソリューションとして多く見られます。しかし、不利な事業上の結果というリスクは、アプリケーションの中に留まるものではなく、アプリケーションそのものに関するリスクよりも大きなものである可能性があります。ユーザーはデータへのアクセスが可能であり、データの保護が事業上必須であることを無視ないしは失念し、たびたびデータをダウンロードし、メールで送付さえする可能性があります。従って、ダウンロードされた重要なデータ資産に係る統制を無視することはできません。ユーザーによるデータ漏洩が管理すべき不利な事業上の結果の重要な一部であれば、そのような統制を無視することはないでしょう。取締役会がIT部門のリーダーに対して、セキュリティリスクの全体像を捉え、個々の技術的な脆弱性の全てに対応するために浪費するのではなく、不利な事業上の結果を管理するための戦略に焦点を当てることを強く求めるべきであるのは、この理由のためです。

4. **サイバー脅威は常に進化している**：サイバー環境における脅威の特質と重大性は絶え間なく変化しているため、脅威のプロファイルに対して常に先手を取るよう、保護対応も進化しなければなりません。定期的な評価は重要ですが、それのみによって管理すべき新たな脅威を特定しようとすべきではありません。取締役会は、組織の現状の脅威管理プログラムが、どのように新たなサイバー脅威を主体的に特定し、それらに対応するのかを問うべきです。その際、自社の最も重要なデータ資産と情報システム、回避したい不利な事業上の結果、業種とビジネスモデルの特質、および潜在的な標的としての知名度を考慮に入れるべきです。また、取締役は、主要なシステム変更から生じる関連するサイバーリスクの評価を行うことを強く求めるべきです。システムの設計にセキュリティを組み込むほうが、後付けで対応するよりも常に低コストで済みます。

5. **サイバーセキュリティはチェスのようなものであり、チェスのように対応すべきである**：ITセキュリティ部門は、サイバー攻撃者よりも数歩先んじ、テクノロジ、人員、プロセス、および技量を武器として構えていなければなりません。実効性と持続可能性のあるセキュリティ・モニタリングのソリューションをテクノロジーのみによって実現しようとする旧来の方法は、今日の常に変化している企業への脅威に太刀打ちできるものではありません。セキュリティ部門は、保護に関するサービスの提供方法を見直し、サイバーリスクの全社的な認知徹底をはるかに超える取り組みを行う必要があります。従って、取締役会は、以下の事項を求めるべきです。

   - 事業の全ての側面（ITだけではなく）が直面している現在のサイバーリスクの明確化。
   - 最近のサイバーインシデント、それらへの対応、および教訓のサマリー。
   - 新たな、より大きな脅威に対応するサイバーリスク対応能力をどのようにして継続的に進化させるのかを、進化を確実なものとするための説明責任の所在を含めてまとめた、短期的および長期的ロードマップ。
   - 現在管理されている最重要サイバーリスクについて、管理の成功度を示す有意義なパフォーマンス指標とリスク指標。[4]

4 そのような指標の例としては以下が挙げられます：現状および目標の成熟度を反映したセキュリティ・プログラムの評価結果、評価を実施した外部ベンダーとサプライヤーの割合、職務分離の不備について評価を実施した高リスク業務プロセスの割合、特定と対応が行われた重大な脆弱性（例：データ漏洩の件数と是正に要したコスト）、月間の高リスク・インシデント件数、インシデントの是正に要する平均時間、特定された監査上および規制上の高リスク課題についての是正状況（例：是正済み件数、未是正件数、および期限超過件数）、およびフィッシング詐欺に関するテストに合格した従業員の割合。

サイバーリスクの管理能力において、現状と目標とする状態の大きな隔たりに直面している組織においては、サイバーセキュリティ・プログラム室を設置し、企業の重要リスクと合致したテクノロジー、人員、およびプロセスに焦点を当てつつ、大規模なセキュリティ・プロジェクトを成功裏に管理するという取り組みが行われ始めています。

6. **サイバーセキュリティは４つの壁を越えて展開しなければならない**：サイバーセキュリティに関する進んだ取り組みが行われている企業と、他の企業の間には、ベンダーのデータセキュリティ管理プログラムと手続きに関する知識において大きなギャップが存在します。組織の最も重要なデータ資産および情報システムと、サイバー攻撃者の間に存在し得る領域においては特にそうです。[5] 上流に位置するベンダーやサプライヤー（サプライヤーの下請けや孫請けを含む）と、下流に位置するチャネル・パートナーと顧客に目を向けるとき、企業は脆弱性の原因を見つけ出すでしょう。電子的なコネクティビティによって社内と社外の区別は不明瞭となっているため、社内リスクの評価を行う際に、取締役は経営者に対して、外部のベンダーやサプライヤーと協力し、バリューチェーン全体にわたる費用対効果に優れたサイバーリスク対応を行うよう求めるべきです。クラウド・ベースのデータ保存や外部データ管理を行うベンダーの利用が増加する中、ベンダーリスク管理の重要性が増しています。

7. **サイバーセキュリティの課題にのみIT予算を振り向けることはできない**：サイバーセキュリティへの対応の適切な実施と、それ対する十分なリソース配分が行われることを取締役会が確保すべきであることに、疑いはありません。しかし、サイバーセキュリティの要請は重要ではありますが、取締役会は自らがイノベーションを抑制してしまうことがないようにすべきです。過去10年にわたって、IT部門は一貫して業務とメンテナンスに係るコスト低減を行い、削減されたコストのほとんどをセキュリティといった他の優先事項に振り向けてきました。プロティビティが行った調査では、コンプライアンスやシステム強化を含む他の優先事項を考慮に入れた場合、成熟した企業においてはイノベーションに振り向けられるのはIT予算全体の13パーセントであることが示されています。[6]

予算が限られる中で、IT部門のリーダーは以下の事項に焦点を当てることが重要になります：第一に、重要なもの（重要なデータ資産や情報システムなど）を保護する、サイバー脅威の状況を常に把握し、発生する見込みが最も高い種類の攻撃を特定する、そして事業への影響を最小化するようシステム復旧を行うために、主体的なインシデント対応を行う。この規律がなければ、サイバーセキュリティはIT予算のより大きな割合を占めるようになるでしょう。その結果としてイノベーションが悪影響を受け、最終的には事業が立ち行かなくなるでしょう。これは、サイバー攻撃が現実のものとなるからではなく、業務リスクに対する過大かつ不必要な支出のために、新たな参入企業および／あるいはイノベーションへの競争的対応における失敗という戦略的リスクから、企業の注意が逸らされてしまうからです。

8. **取締役は自らが受けている助言にどの程度の信頼をおいているかを把握すべきである**：全ての企業に当てはまるソリューションは存在しませんが、取締役会は、サイバーセキュリティ事項に関して自らが頼りにしている専門的知識が十分であるかを、定期的に評価すべきです。状況によっては、特に取締役会が多くの議題を抱えている場合には、取締役会は、テクノロジに関する経験を有する個人を取締役会のメンバーあるいは取締役会の顧問として迎えるべきであるかを積極的に検討すべきです。

企業がグローバル戦略を実行する上でテクノロジーへの依存を高める中で、サイバーセキュリティは今後も長く最重要リスクであり続けるでしょう。現実のサイバーリスク管理においては、サイバーリスクを除去することは不可能であり、リソースは限られており、リスク・プロファイルは常に変化し、確実な安全性は容易に確保できるものではありません。このため、保護対応に関する投資の対象を、組織の最も重要なデータ資産と情報システムに対して不利な影響を与え得る事業上の結果に絞ること、変化し続ける脅威の状況とリスク許容度を理解すること、および必ず発生するインシデントに備えることが重要です。

5 Managing the Crown Jewels and Other Critical Data, Protiviti, 2017 (www.protiviti.com/US-en/insights/it-security-survey)

6 From Cloud, Mobile, Social, IoT and Analytics to Digitization and Cybersecurity: Benchmarking Priorities for Today's Technology Leaders, Protiviti, 2016 (www.protiviti.com/sites/default/files/united_states/insights/annual-technology-trends-and-benchmark-study-2016-protiviti.pdf)

取締役会の考慮事項

以下は、事業体の活動に内在するリスクに関連して取締役会が考慮すべき事項です。

- 取締役会として、サイバーセキュリティの監視に十分に関与しているか、例えば
  - » サイバーセキュリティを組織にとって中心的なリスクと捉え、取締役会への適切な状況報告を求めているか。
  - » サイバーセキュリティについて中心的な役割を担う取締役会メンバーまたは顧問が存在するか。
  - » セキュリティ・インシデントのリスクを許容水準にまで低減するための自社の戦略は適切であり、焦点の絞られたものであるか。
  - » 取締役会は、セキュリティ・プログラムの現状を客観的に表した主要指標または報告を受領しているか。
  - » 取締役会資料およびその他センシティブな資料の取締役への送達における安全性確保に関する方針が定められているか。定められていない場合には、自社のサイバーセキュリティ・インフラがカバーしていない、取締役が個人的にまたは職業上使用しているメールアカウントや無償のファイル共有サービスを通じて、機密情報を共有することから生じる潜在的なエクスポージャーは存在するか。
- 重要なデータと情報システムに関係する、最も重要な事業上の結果（デジタル化の取り組みにおける予期せぬ成功と、不利な事象の両方）を特定しているか。これらの結果の発生に関して、以下の事項を考慮しているか。
  - – 最も重要な事業上の結果について管理が行われているか、およびどのように管理が行われているかを把握しているか。
  - – 自社のセキュリティ戦略において、それらをサイバーセキュリティ全般から区別しているか。
  - – これらの事項に関する脅威の状況と許容度を定期的に評価しているか。
  - – 新たなサイバー脅威の特定と対応を主体的に行っているか。
- 自社はインシデント対応計画を備えているか。計画を備えている場合には、以下の事項を考慮しているか。
  - – 主要なステークホルダーは、自社の規模、文化、適用される規制上の義務[7]、および事業目的に適した計画の策定を支援しているか。
  - – 具体的なサイバー事象が自社に与える影響と、経営者の対応計画の方向性が適切であり、十分に支援されているかについて検討しているか。
  - – 具体的な種類のインシデントへの対応において取るべき行動に関するインストラクションを示した手続きによって、対応計画の補完が行われているか。計画されている対応に関係するすべてのステークホルダーは、それぞれの役割と責任を認識しているか。どの事象について、対応の取り組みの監視において取締役会が主要な役割を担うべきであるのかが明確であるか。
  - – セキュリティ侵害の発生、拡散および影響を低減するための有効なインシデント対応プロセスが整備されているか。
  - – 対応計画の有効性を判断するために、主体的かつ定期的な評価とテストを実施しているか。例えば、経営者は定期的にシミュレーションを実施し、最新の攻撃手法を検知する能力が備わっているかを確認しているか。
  - – 過去の重大なデータ侵害が発生した際に、適用法令と規制に従い、公衆に対して求められる開示、ならびに規制当局および法執行当局への適切な通知を行ったか。

プロティビティの支援

プロティビティは企業と共に、以下の様な根本的な情報セキュリティの課題に焦点を当てています。

- 何を保護する必要があるのかを認識しているか（例えば、最も重要なデータと情報システム資産）、それらはどこに存在するか。それらの資産について以下の事項を考慮しているか。
  - – それらの資産を十分に保護しているか。何によってそのことを確認できるか。
  - – 誰からそれらの資産を保護しているのか、誰に対してそれらの資産へのアクセスを許可すべきか、アクセスを許可すべき者とそうではない者をどのように区別できるか。
  - – 保護の仕組みは有効であるか。設計されたとおりに機能しているか。
  - – 計画どおりに物事が行われていない場合に、どのようにしてそのことを把握するのか。
- 自社の環境に対する新たな脅威の認識と想定される攻撃手法の検知を適時に行い、脅威に合致するよう保護の仕組みを見直しているか。
- よからぬことが起こった際に対応する準備ができているか。そのようなインシデントを管理する能力を有しているか。インシデントが発生した際に、その再発を防ぐことができるか。

プロティビティは、幅広い種類のセキュリティとプライバシー評価、アーキテクチャ、トランスフォーメーションと管理に関するサービスを提供し、セキュリティとプライバシーに関するエ

7 例えば、米国においては、金融機関を対象としたグラム・リーチ・ブライリー法や、健康情報に関する医療保険の携行性と責任に関する法律（HIPPA）法、決済サービスに関するPCIセキュリティ基準、など。

クスポージャー（例えば、顧客データの喪失、収益の喪失、あるいはレピュテーションの低下）を未然に特定し対応する上での企業の支援を行っています。プロティビティは、全ての業種の企業と共に、情報セキュリティ・プログラムの成熟度や統制の有効性を評価し、必要である場合には改善策の策定と実施を支援しています。セキュリティ・インシデントへの対応、主体的なセキュリティ・プログラムの確立、個人情報とアクセス管理対応、および業種に特有のデータセキュリティとプライバシーの課題への対応における企業の支援に関して、プロティビティは、確たる実績を有しています。世界クラスのインシデント対応における経験と専念により、プロティビティはセキュリティ戦略、対応実施、フォレンジック分析、および対応計画策定における深い専門知識を有しています。

Board Instituteが取締役会のリスク監視の新たな評価ツールを公開

TBI Protiviti Board Risk Oversight Meterは、取締役会が自らのリスク監視プロセスを見直し、真に重要性のある機会とリスクに焦点を絞ることを確実にする機会を提供するものです。プロティビティは、企業が自信を持って未来に立ち向かうための継続的なプロセス改善を促進することにコミットしており、柔軟で費用対効果に優れたツールを提供するためにBoard Instituteと協力しています。このツールは、取締役会が自らのリスク監視について行う定期的な自己評価を支援するものであり、多くの取締役が好ましいと考える自己評価のあり方を反映したものです。

詳しくはこちら：www.protiviti.com/boardriskoversightmeter